# 編輯序

資訊安全通訊期刊本季Vol. 27 No. 2以電子刊物與印刷的刊物形式並行發行，本會會員將以電子刊物的形式發放，紙本印刷期刊發行予團體及機關訂戶。

本期卷公開徵稿部分收錄了三篇文章，分別為臺北市立大學資訊科學系壽大衛教授及其研究團隊撰寫之「以區塊鏈技術建立具有履約保證機制的遞延性商品(服務)平台：以補教業為例」、國立中興大學資訊管理學系林詠章教授及其研究團隊撰寫之「智慧合約於分散式金融應用之漏洞攻擊解析與解決方案」以及高雄醫學大學醫務管理暨醫療資訊學系陳以德教授及其研究團隊撰寫之「以屬性加密為基礎的輕量化雙向認證」。

「以區塊鏈技術建立具有履約保證機制的遞延性商品(服務)平台：以補教業為例」一文針對遞延性商品(由消費者先預付費用才獲得服務)進行研究，該解決方案於銀行建構聯盟區塊鏈，套用補教業場景，建構模型以從技術上展示該平台的運作模式，打造更具安全性、公信力及合法的交易平台。「智慧合約於分散式金融應用之漏洞攻擊解析與解決方案」探討目前各項分散式金融(DeFi)協議的技術，利用目前各類常見DeFi應用可能產生之漏洞進行攻擊解析，包含閃電貸、預言機、治理項目等應用，針對Unstoppable、Naive Receiver、Truster、Side Entrance、The Rewarder、Selfie、Compromised及Puppet等八種可能漏洞進行攻擊解析，進而提供智慧合約安全之撰寫或解決方式。「以屬性加密為基礎的輕量化雙向認證」以屬性加密(Attribute-based Encryption)為主要架構，使用者可以選擇符合病患的屬性特徵以制定一些存取規則(Access policy)，病患數據只能夠被某些符合其存取規則的特定使用者存取，其他無法滿足存取規則的使用者即使竊取到了數據，也因為透過加密而無法取得其明文內容。

在本期 Quarterly 部分，收錄了團體會員簡介，提供各位會員參閱。本刊將持續朝落實期刊國際化與開放取用(Open Access)工作方向邁進，陸續著手國際知名研究索引資料庫的申請工作，感謝所有讀者長期的支持，並歡迎各位先進提供最新的研究成果至本刊進行分享與交流。

國立宜蘭大學
資訊工程學系
陳 麒 元